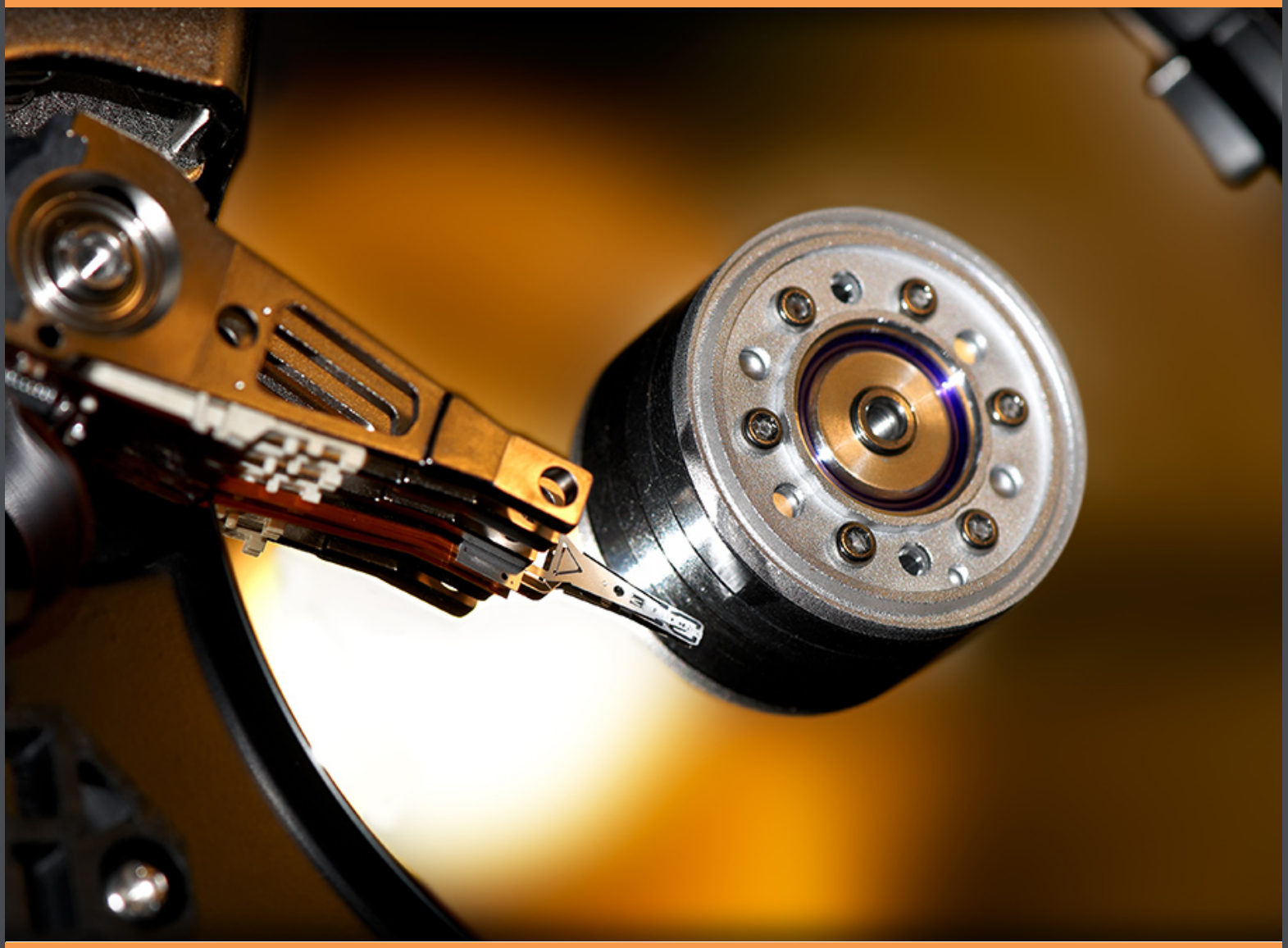
Business Information Systems

Elizabeth Hardcastle



Elizabeth Hardcastle

Business Information Systems

Business Information Systems

ISBN 978-87-7681-463-2

Contents

1 Defining Information Systems

This chapter provides a discussion of the nature of information and systems.

1.1 Defining Data and Information

It is important to distinguish between data and information. Data is a raw fact and can take the form of a number or statement such as a date or a measurement. It is necessary for businesses to put in place procedures to ensure data are recorded. For example, to ensure a call centre operator includes the postcode of every customer this can be written into their script and a validation check performed to check these data have been entered into the system.

A common definition of information is that it is data that have been processed so that they are meaningful (Oz and Jones, 2008). This requires a process that is used to produce information which involves collecting data and then subjecting them to a transformation process in order to create information. Some examples of information include a sales forecast or a financial statement.

As stated information is generated through the transformation of data. This can be achieved using a number of different transformation or data processes. Some examples of data processes include aggregating which summarises data by such means as taking an average value of a group of numbers. Classification places data into categories such as on-time and late deliveries. Sorting organises data so that items are placed in a particular order, for example listing orders by delivery date. Calculations can be made on data such as calculating an employee's pay by multiplying the number of hours worked by the hourly rate of pay. Finally data can be chosen based on a set of selection criteria, such as the geographical location of customers.

Although information is an useful resource for individuals and organisations not all information can be considered useful. The differences between 'good' and 'bad' information can be identified by considering whether or not it has some or all of the attributes of information quality. Attributes can be related to the timing, content and form of the information.

Timeliness refers to that the information should be available when needed. If information is provided too early, it may no longer be current when used. If the information is supplied too late, it will be of no use. Also the information should cover the correct time period. A sales forecast, for example, might include information concerning past performance, current performance and predicted performance so that the recipient has a view of past, present and future circumstances.

The content of the information refers to factors such as the accuracy of the information and relevance of the information to a particular situation and user.

The form of the information refers to aspects such as the clarity of the information which should be appropriate to the intended recipient. The recipient should be able to locate specific items quickly and should be able to understand the information easily. The information should also contain the correct level of detail in order to meet the recipient's information needs. For example, in some cases highly detailed information will be required whilst in others only a summary will be necessary.

1.2 Defining Systems

A system can be defined as a collection of components that work together towards a common goal. The objective of a system is to receive inputs and transform these into outputs. In the previous section 'defining data and information' the use of a transformation process was used to explain how data is converted into information. Not every system has a single goal and often a system contains several subsystems with subgoals, all contributing to meeting the overall system goal. For example the finance, operations and marketing areas of an organisation should all have goals which together help to achieve overall corporate objectives. It can be seen that in systems data are used as the input for a process that creates information as an output. In order to monitor the performance of the system, some kind of feedback mechanism is required. In addition, control must be exerted to correct any problems that occur and ensure that the system is fulfilling its purpose. There are thus five components of a generic system in terms of input, process, output, feedback and control.

1.3 Defining Information Systems

The role of the Information systems to provide information to management which will enable them to make decisions which ensure that the organisation is controlled. The organisation will be in control if it is meeting the needs of the environment. In relation to control systems can be classified into open-loop and closed-loop (Bocij et al., 2008).

An open-loop control system is one that has no way of ensuring objectives are met for a process. This means they are unsuitable in an organisational context because of the complexity of the environment in which organisations exist. Thus open-loop systems would only be successful in attaining a system's objectives in cases where we know with certainty the events that would take place during the system's process.

Closed loop systems can have two types of control mechanism referred to as feedback control and feedforward control. Feedback control systems generally provide a way of ensuring a system is under control. Negative feedback is when actions are taken to reverse any differences between desired and actual outputs. The weakness of this approach is the potential for delay between the discrepancy and the action taken to reduce it. Feedforward control systems attempt to overcome the time-delay associated with feedback systems by incorporating a prediction element in the control feedback loop. Feedforward systems are not as common as feedback systems in business settings. Examples include project management plans which are made to meet time, quality and cost objectives over time.

1.4 Business Information Systems

With the previous definitions of information and systems we can now define a business information system as a group of interrelated components that work collectively to carry out input, processing, output, storage and control actions in order to convert data into information products that can be used to support forecasting, planning, control, coordination, decision making and operational activities in an organisation (Laudon and Laudon, 2007). In terms of the components that undertake this activity, they can be classified into five basic resources of people, hardware, software, communications and data. People resources include the users and developers of an information system and those who help maintain and operate the system such as IS managers and technical support staff. Hardware resources include computers and other items such as printers. Software resources refer to computer programs known as software and associated instruction manuals. Communications resources include networks and the hardware and software needed to support them. Data resources cover the data that an organisation has access to such as computer databases and paper files.

In most organisations Business Information Systems (BIS) make extensive use of information technology, such as personal computers. The reasons why computerised BIS have become widespread are evident in their advantages such as speed, accuracy and dependability. They also have a high degree of flexibility due to their ability to be programmed to carry out a wide variety of tasks. There are, however, some disadvantages to BIS such as their lack of creativity that humans possess and the difficulty of incorporating other factors into their decision making such as innovation and intuition.

1.5 Types of business information system

Information systems may be divided into two categories of systems that support an organisation's day-to-day business activities and systems that support managerial decision making. Operations Information Systems (OIS) are generally concerned with process control, transaction processing and communications. Management Information Systems (MIS) are concerned with providing support to managerial decision making. Recently this division of BIS into operational and management systems, although useful for managers reviewing the types of BIS in use, does not now accurately reflect the reality of systems used within an organisation, particularly with the increased use of inter-organisational e-commerce and electronic data interchange (EDI). For example e-business systems and enterprise resource planning systems cut across both operational and management systems to provide businesses with more integrated information systems.

2 Hardware

Hardware describes the physical components of a computer system which can be categorised as input devices, a central processing unit, internal and external memory and output devices (Beynon-Davis, 2009). Input devices are used to capture or enter data into the computer. The central processing unit (CPU) performs processing by carrying out instructions given in the form of computer programs. Internal memory is used as a temporary means of storage data and instructions while external memory provides a means of storing data and programs outside of the computer. Output devices translate the results of processing into a human-readable form. These hardware components will now be described in more detail.

2.1 Input devices

Input devices are used to enter data or instructions from outside the computer into the computer. A mouse and keyboard are examples of input devices. The choice of an input device will often depend upon the quantity of data to be entered. Entering data on a small scale is normally carried out by human operators, using a number of familiar input devices, such as the mouse or keyboard. A computer-based information system will seldom make use of only a single input device. Even a typical personal computer will often feature several different methods for data entry, such as keyboard, mouse, joystick and sound card.

2.2 Central Processing Unit (CPU)

The central processing unit (CPU) or processor accepts instructions and data and executes them storing the results in memory. The increased speed of computers is primarily a result of increasing CPU speeds. The speed of a processor will depend upon a number of different factors. such as the clock speed and bus width. The clock speed determines how many instructions per second the processor can execute. The bus width describes how many pieces of data can be transmitted at one time. In both cases the higher the value, the more powerful the processor. Clock speed and bandwidth values can be helpful when attempting to compare processors in order to select the most appropriate.

2.3 Internal and External Memory

Computer memory is categorised as internal memory (also called main memory or primary memory) which is data held on the computer and external memory (also called external storage) which is data stored on a separate device where the information will be retained even if the machine is switched off. Computer memory is used to store data awaiting processing, instructions loaded from software which are used to process data or control the computer system and data or information that has been processed. Floppy and hard disks are examples of external memory.

2.4 Output devices

Output devices display the results of computer processing. A computer-based information system will make use of a number of output devices as a monitor, printer and sound card.

2.5 Major categories of computers

There are three basic categories of computer: mainframe, minicomputer and microcomputer. We will briefly examine the characteristics of each category, in order to understand more of how industry makes use of computer technology.

2.5.1 Mainframe

Mainframe computers have been traditional associated with large, powerful machines designed for large-scale data-processing activities. The use of mainframe computers in industry, once responsible for the large revenues of companies such as IBM has declined steadily over the past two decades. IBM, Fujitsu and Unisys are current suppliers. Advances in technology have enabled smaller, less expensive systems to compete with mainframes in terms of speed and power. A modern personal computer, for example, could be considered many times more powerful than one of the very earliest mainframe systems. In many organisations, mainframe computers are considered legacy systems, meaning that while managers recognise that the existing system may not be entirely adequate to meet the company's needs, a changeover would be difficult to implement.

2.5.2 Minicomputers

The minicomputer combines some of the characteristics of the mainframe computer and the microcomputer. Today, they are often referred to as servers by companies such as IBM (e.g. the IBM AS/400) and Hewlett-Packard (e.g. HP Alpha). Different types of server may have different functions, such as managing a network or hosting a database.

2.5.3 Microcomputers

The microcomputer makes use of more modern technology to provide relatively powerful computing facilities at low cost. Microcomputers are now often referred to as the 'client' machine which receives services and data from a 'server' machine. Some of the major characteristics of the microcomputer are that they a re small, relatively inexpensive and can be used for a variety of purposes.

3 Software

This chapter provides a review of the features common to a range of modern software applications, and the way in which software can be used to support the business activities of an organisation. Software can be defined as a series of detailed instructions that control the operation of a computer system and exists as *programs* which are developed by computer programmers. There are two major categories of software of systems software and applications software (Laudon and Laudon, 2007).

3.1 Systems software

Systems software manages and controls the operation of the computer system as it performs tasks on behalf of the user. Systems software consists of three basic categories: operating systems, software development programs and utility programs.

3.1.1 Operating Systems (OS)

The operating system interacts with the hardware of the computer by monitoring and sending instructions to manage and direct the computer's resources. The operating system functions as an intermediary between the functions the user needs to perform, for example a database search, and how these translate to and from the hardware in the form of responding to mouse clicks and displaying information on the screen. The basic functions of the operating system include: allocating and managing system resources, scheduling the use of resources and monitoring the activities of the computer system.

3.1.2 Software Development programs

Software development programs allow users to develop their own software in order to carry out processing tasks using programming languages. Programming languages can be described in terms of their historical position in the development of computer programming systems. The first generation programming language or machine language requires a programmer to work in one and zeros to represent characters and numbers. This extremely time consuming tasks was somewhat simplified using shorter codes and called assembly language. A major advance came with third generation languages such as FORTRAN, COBOL, BASIC ,Pascal and C which substantially reduce the programmer's time in producing code. Fourth generation languages such as SQL are built around a database system and make producing code even easier than third generation languages.

3.1.3 Utility programs

Utility programs provide a range of tools that support the operation and management of a computer system. Programs that monitor system performance or provide security controls are examples of utility programs.

3.2 Application software

Application software can be defined as a set of programs that enable users to perform specific information-processing activities. Application software can be divided into two broad categories: general-purpose and application-specific.

3.2.1 General-purpose applications

General-purpose applications are programs that can be used to carry out a wide range of common tasks. A word processor, for example, is capable of producing a variety of documents that are suitable for many different purposes. This type of application is often referred to as productivity software since it helps improve the efficiency of an individual. Word processing software involves the creation of various internal and external documents, including letters, reports, invoices, notes and minutes of meetings. Spreadsheet software enables the storage, organisation and analysis of numerical data. Databases software allows for the storage and retrieval of information. Multimedia software allows the user to work with media such as text, sound, animation and video.

3.2.2 Application-specific software

Application-specific software comprises programs intended to serve a specific purpose or carry out a clearly defined information processing task. Software designed to carry out payroll processing or manage accounts is an example of an application-specific program.

4 Database Systems

The purpose of a database is to keep track of things (Kroenke, 2007). Databases can exist on paper, for example a telephone directory, but are inefficient and costly to maintain. A computer-based database offers the advantage of powerful search facilities which can be used to locate and retrieve information many times faster than by manual methods. An electronic database provides facilities for users to add, amend or delete records as required. Indexing features mean that the same basic information can be stored under a number of different categories. This provides great flexibility and allows users to locate, retrieve and organise information as needed. Databases used throughout a company are usually accessed by many different users across a network system. Some of the advantages of this approach include minimising the unnecessary duplication of information, consistency is maintained by ensuring any changes made to the information held in the database are reflected to all users and although information is held in a structured manner, the database software will normally provide sufficient flexibility to meet the different requirements of individual users and departments.

4.1 Organising data in a database

The data in an electronic database is organised by fields and records. A field is a single item of information, such as a name or a quantity. A record is a collection of related fields and a table is a collection of related records. In order to identify a specific item of information within a database, all records must contain a unique identifier, normally called the key field or primary key. The key field usually takes the form of a number or code and will be different for each record in the database.

Relational databases enable data to be stored within a number of different tables and are the most widely used type of database. The tables within a relational database can be linked together using one or more record keys. This include the primary key and also other keys to help locate data stored in another table. The record keys contained in each table can used to establish one or more relationships between tables. By using record keys in combination it is possible to retrieve data from several tables at once. The field used to locate information in another, related table is often called a foreign key.

4.2 Database Software

The majority of database programs support the creation of relational databases containing several linked tables. Many programs, such as Microsoft Access, provide the ability to link tables together automatically to create any required relationships. All major database programs enable users to create and modify data entry forms. A data entry form provides a convenient means of viewing, entering, editing and deleting records. An index stores information concerning the order of the records in the database. All modern database programs provide a range of sophisticated security features. Examples of some of the most common features available including encryption and password protection. Finally all major database packages allow users to generate a wide variety of reports. Many programs are capable of creating simple reports automatically. In addition, many programs allow users to perform calculations and other actions as the report is produced.

4.3 Retrieving Data from a Database

When using database software data is retrieved from a database using what is called a query. A query enables a user to locate, sort, update or extract records from the database. Users design a query by specifying the conditions that must be met in order for a record to be selected. There are two types of query called selection queries and update queries: A selection query can be used to locate and display any records meeting a set of specified conditions. None of the data held in the database are altered and any records not meeting the conditions set are simply hidden from view temporarily. An update query can be used to modify records in a variety of ways such as according to a set of conditions specified by the user. Common actions performed by update queries include updating values held in fields, deleting any records no longer required, appending new records to the database and generating new tables containing selected records or summary information.

The majority of database programs make use of a special structured query language (SQL) in order to create queries. Structured query language (SQL) provides a standardised method for retrieving information from databases. Although traditionally used to manage large databases held on mainframes and minicomputers, it has become a widely used and popular tool for personal computer database packages. SQL programs are created by producing a series of statements containing special key words.

4.4 Business Intelligence

Business Intelligence (BI) systems are needed due to the vast amounts of data now held in organizational information systems and the need to extract useful information from this in the form of patterns, trends and present this in a understandable way to decision makers. BI systems generally focus on providing timely information at a strategic level in large organizations with large data sets (hence the need for a data warehouse described later). BI systems also generally provide indirect support for particular decisions rather than the decision specific orientation of decision support systems.

A BI system has four major components of a data warehouse, business analytics, business performance management (BPM) and user interface (Turban et al, 2010). Data is gathered from various sources and then held in a special database repository termed a data warehouse in order to support decision-making in the organisation. Repositories of data focused on departmental or subject areas are termed data marts. Data mining is a type of analysis that aims to identify patterns in the data that can be used to predict future behaviour. Business Analytics are used to conduct analysis of the data held in the data warehouse using reporting and querying tools. Business performance management covers the methodologies used to measure and manage business performance. The user interface integrates and displays information from multiple business areas. Dashboards provide a visual representation in the form of graphs comparing actual performance to desired performance targets.

5 Networks

A network links two or more computers to share data or resources (Laudon and Laudon, 2007). This allows people to collaborate and also allows hardware such as printers and faxes to be shared more cost-effectively.

Networks are important to an organisation because they help a business connect with its customers, suppliers and collaborators. Through doing this a company can order new raw materials more rapidly and cheaply from its suppliers and can keep in touch with the needs of its customers. Further benefits of networks include reduction of costs through the use of facilities such as email, reduced time for information flow, for example comparing email with post delivery, ability to share information by accessing a database over a network system, ability to share hardware devices such as printers over a network, use of group working tools to share documents and other information. The main disadvantages of networks are the cost of installing the network and ensuring a secure and reliable network service.

5.1 Network components

Some of the major components that make up a network are now described.

5.1.1 Servers

Servers control the flow of information around the network and use specialised software called the network operating system (NOS) to manage the network. The server and NOS together enables sharing of information, application software and hardware devices such as printers. It also controls access to information in files. For a network of perhaps 20 people or more, the functions described above may be split between several servers to share the load. There may be a separate file server, print server, password server and database server. In very large companies there will be many servers used for data storage. These will all be linked by the network to ensure that the data are accessible by everyone. They will also be responsible for ensuring through a process known as replication that the same version of data exists on different servers. With the use of many servers, an opportunity exists to spread the computing workload across these servers rather than overloading a single central machine, which happened in the days of the mainframe. The sharing of functions across several computers is known as 'distributed computing'.

5.1.2 End-user computers or terminals

The access points for users of a network are known variously as clients, nodes, work- stations or, most commonly, PCs. To work on the network each client must have networking software such as Novell Netware installed. A connection to the network is also required through either a network cable connected to a network interface card in one of the PC's slots or through a wireless network system.

5.1.3 Telecommunications processors

Telecommunications processors are the pieces of hardware that are used to link the servers and clients and different networks together. These are usually referred to by their specific names, such as hubs, multiplexers, bridges and routers. In a company that needs to use gateway devices, a specialist is required to maintain them. Hubs are used to connect up to 20 PCs to a network in a convenient way using patch cables (which look similar to phone cables and sockets) running between the back of each PC and the hub. The hub may then be attached to a server or a backbone connection leading to the server. Routers can select the best route for packets to be transmitted and are also used on the Internet backbones and wide area network to achieve this. Although these devices used to be distinct, they are now produced as hybrids which share functions. Companies attached to the Internet usually use a router as a gateway to attach their internal network to the Internet. This is often combined with a 'firewall', which is intended to reduce the risk of someone from outside the company gaining unauthorised access to company data.

5.1.4 Middleware

Middleware is a specialised type of software which allows different software applications to communicate. It acts as a layer between other software to assist in data transfer between incompatible systems. It is often described as the 'glue' that binds the software applications to the systems software. It is important in a networked world, since it provides translation services between software running on different types of computer systems in different companies. An example of middleware is gateway software which enables an internal e-mail system such as Lotus cc:Mail to send messages to other e-mail systems via the Internet. Middleware is also necessary to enable a single software application such as sales order processing to access different types of database, such as Oracle, Informix or Microsoft SQL Server, which a large company may use. Middleware to assist in communications can be categorised according to a seven-layer model known as the OSI model.

6 The Internet and World-Wide Web

The Internet is a vast network of computers connected across the globe that can share both information and processing (Oz and Jones, 2008). Information is transmitted from PCs whose users request services to computers that hold information and host business applications that deliver the services in response to requests. The PCs within homes and businesses are connected to the Internet via local Internet service providers (ISPs) which, in turn, are linked to larger ISPs with connection to the major national and international infrastructure or backbones. The Internet can be described is as a global network system made up of smaller systems. The Internet was conceived by the Defense Advanced Research Projects Agency (DARPA), an American intelligence organisation, in 1969. The Internet began to achieve its current form in 1987, growing from systems developed by DARPA and the National Science Foundation (NSF).

6.1 Web-Enabled Business

Web-enabled business can be classified by those parties involved in business transactions. The most common transactions identified as those when an organisation is using the Internet to transact with consumers, termed business-to-consumer (B2C) or when an organisation is transacting with other businesses, termed business-to-business (B2B). The relationship between a company and its suppliers and customers can be dramatically altered by the opportunities afforded by the Internet. This occurs because the Internet offers a means of bypassing some of the channel partners. This process is known as disintermediation or 'cutting out the middleman'. The benefits of disintermediation are that it is able to remove the sales and infrastructure cost of selling through the channel. Some of these cost savings can be passed on to the customer in the form of cost reductions. Although disintermediation is widespread the creation of new intermediaries between customers and suppliers, termed re-intermediation, has also occurred. For example in the travel industry companies such as Tripadvisor provide information regarding destinations and hotels and then provide links to hotel providers.

6.2 Intranets and extranets

The majority of Internet services are available to any business or consumer that has access to the Internet. However, many business applications that access sensitive company information require access to be limited to favoured individuals or third parties. If information is limited to those inside an organisation the network is termed an intranet. If access is extended to some others, but not everyone beyond the organisation, the network is termed an extranet (Laudon and Laudon, 2007). Extranets can be accessed by authorised people outside the company such as collaborators, suppliers or major customers, but information is not available to everyone with an Internet connection but restricted using password access. Intranets are also used for sharing information such as staff phone directories, staff procedures or quality manuals, information for agents such as product specifications, current list and discounted prices, competitor information, factory schedules and stocking levels – all this information normally has to be updated frequently and can be costly. Extranets are used extensively to support activities such as ordering from suppliers.

6.3 The World Wide Web

The World Wide Web provides a standard method for exchanging and publishing information on the Internet. The medium is based on standard document formats such as HTML (hypertext markup language) which has been widely adopted because it supports a wide range of formatting facilities making documents easy to read on different access devices. It also incorporates graphics and animations which can be integrated into web pages and interaction is possible through HTML-based forms that enable customers to supply their personal details for more information on a product, perform searches, ask questions or make comments.

It is the combination of web browsers and HTML that has proved so successful in establishing widespread business use of the Internet. The use of these tools provides a range of benefits such as increasing the ease to which navigation between documents is enabled by the use of hyperlinks or images. This soon becomes a very intuitive way of navigation which is similar across all web sites and applications. It can provide a graphical environment supporting multimedia which is popular with users and gives a visual medium for advertising. The standardisation of tools and growth in demand means information can be exchanged with many businesses and consumers.

6.4 Web browsers and servers

Web browsers are software applications that are used to access the information on the world wide web that is stored on web servers. Web servers are used to store, manage and supply the information on the world wide web. The main web browsers in use are Microsoft Internet Explorer and Mozilla Firefox. Browsers display the text and graphics accessed from web sites and provide tools for managing information from web sites.Web browsers communicate with web servers in the following way. A request from a PC is executed when the user types in a web address, clicks on a hyperlink or fills in an online form such as a search. This request is then sent to the ISP and routed across the Internet to the destination server using the mechanism described in the section on protocols. The server then returns the requested web page if it is a static (fixed) page, or if it requires reference to a database, such as a request for product information, it will pass the query on to a database server and will then return this to the customer as a dynamically created web page. Information on all page requests is stored in a transaction log file which records the page requested, the time it was made and the source of the enquiry.

6.5 E-business

E-business involves several key activities including improving business processes, enhancing communications and providing the means to carry out business transactions securely. E-business is part of a broader Internet economy which encompasses all of the activities involved in using the Internet for commerce. The Internet economy is made up of the following layers:

- Internet Infrastructure. Companies that provide the hardware, software and other equipment for the Internet. Examples: ISPs, networking companies and manufacturers of PCs and servers.

- Internet Applications Infrastructure. Companies that provide software facilitating Internet transactions. Also, companies that provide web development, design and consulting services. Examples: producers of web development software, web-enabled databases and search engines.

- Internet Intermediaries. Companies that link buyers and sellers, for example by providing content or by creating marketplaces where business can be transacted. Examples: travel agents, content providers and online brokerages.

- Internet Commerce. Companies that sell products and services to consumers or other companies. Examples: online retailers, subscription or fee-based services and manufacturers selling directly to the public.

In general, the benefits of e-business include reduced costs, improved efficiency and access to larger markets. By automating many of the administrative tasks associated with ordering, supplying and delivering goods or services, the cost of a typical business transaction can be reduced significantly. E-procurement is used to reduce administrative costs and purchase goods at lower prices. It was mentioned earlier that adopting an e-business approach could help to enhance three main areas of business: production processes, customer-focused processes and internal management processes. In terms of customer-focused processes, for example, the efficiency of customer services can be improved through the introduction of a help desk on the company's web site. As well as helping customers, such a facility can also act to reduce costs by reducing pressure on other support services, such as telephone helplines. Finally, the adoption of an e-business approach can help companies to reach a larger, global market. This is often one of the benefits of restructuring the relationship between manufacturer, retailers and customers.

6.6 E-commerce

A common activity associated with e-business is e-commerce which can be described as using technology to conduct business transactions, such as buying and selling goods and services. However, e-commerce involves more than merely conducting electronic transactions; it also encompasses a wide range of associated activities, such as after-sales support and even logistics.

E-commerce activities can be broken down into five basic types:

- Business-to-business (B2B). Transactions take place between companies. Approximately 80 per cent of all e-commerce is of this type.

- Business-to-consumer (B2C). Companies sell products directly to consumers. B2C can involve activities such as product research (where consumers gather information and compare prices) and electronic delivery (where information products are delivered to consumers via e-mail or other means).

- Business-to-government (B2G). Transactions take place between companies and public sector organizations.

- Consumer-to-consumer (C2C). Transactions take place between private individuals. Perhaps the best examples of C2C commerce are online auction sites and peer-to-peer systems.

- Mobile commerce (m-commerce). M-Commerce is a relatively new development and involves selling goods or services via wireless technology, especially mobile phones.

7 Acquiring Information Systems

The main choices when acquiring information systems can be categorised as off-the-shelf (packaged), bespoke applications developed by an in-house IT department or a software house and end-user developed systems (Bocij et al., 2008).

7.1 Bespoke development

Bespoke development refers to when an information system is developed by an information systems professional to match the business requirements of the application. The information systems professionals will either work for the business which is termed 'in-house' bespoke development or for a third party such as a software house which is termed 'outsourced' software development. Bespoke development has the benefit of producing software tailored to the precise requirements of the business. Disadvantages include cost, bespoke development is the most expensive way of developing new information systems. In terms of time bespoke development, especially when using formal structured development methodologies, is notorious for time overruns, with delays of months or years not uncommon and quality. Finally in terms of quality bespoke software is not usually free from bugs; software bugs can range from the trivial to the catastrophic, the latter often attributable to poor analysis of requirements.

7.2 Off-the-shelf software

Off-the-shelf purchase of packaged software is an acquisition method that involves direct purchase of a pre-written application used by more than one company. This type of software is pre-written and is available for a whole variety of hardware platforms from PCs to mainframes. Off-the-shelf software is written to offer a broad functionality that will suit a wide range of different businesses. This broad range of functions has the benefit of fitting the requirements of a large number of businesses. It also may offer too many features for any particular business, which may then feel that it is paying for things it will not use. At the same time, it may require businesses to process information in a particular way that is at odds with the way they normally do business. Alternatively, a certain off-the-shelf software package may not offer sufficient features. The major benefit, however, of off-the-shelf software packages is their low cost when compared with acquiring bespoke software with the same level of functionality. In addition, because packaged software has been developed for a commercial market, it is less likely to suffer from the bugs that afflict bespoke software. In a tailored off-the-shelf purchase, pre-written software is purchased from a supplier, but it is possible to configure it to be specific to the company. In a component off-the-shelf purchase, different modules may be purchased from different suppliers and built together.

7.3 End-user-developed software

End-user-developed software is software written by non-IS professionals, i.e. the business users.

Enterprise resource planning or institutional applications are those that affect general corporate activities, cut across more than one department or functional area, or systems that involve organisational data held in corporate databases. Examples include accounting systems, sales order processing systems and materials requirements planning. End-user applications are more limited in scope. Applications may be departmental or personal in nature and are usually output- or report-oriented rather than input-driven. These applications may either be written by IT professionals or by the end-users themselves. If the latter is the case, they are often referred to as end-user-developed applications. Such systems may be simple such as a spreadsheet or a small PC database or less commonly they may be more sophisticated such as a production planning system based on sales forecast data from several branches of the same organisation. Such applications are typically for individual or departmental use, although in the case of the second example the system may have company-wide relevance. The main benefit of end-user-developed software is that it is normally used by those who develop it, and so the requirements are not subject to mistranslation or the provision of over-sophisticated solutions. The negative side to this is that in some cases inappropriate software development tools might be used such as complicated spreadsheets instead of the construction of a database. A further significant concern with end-user development is that software may be riddled with bugs as a consequence of corner cutting such as poor or non-existent design, little or no testing, or no documentation.

There are also a number of hybrid approaches to acquisition. A group of organisations in the same business or activity area may have information systems requirements that individually may be very expensive to develop. A solution may be for a bespoke system to be developed by a third party, which allows the development costs to be spread among all the organisations involved. Similarly, an off-the-shelf package may provide 80 per cent of the required features, but others may need to be added through some bespoke development by either IS/IT professionals or by end-users. The approaches to systems acquisition described above are not mutually exclusive for a given project or within an organisation. Where the software is generic to all businesses, as is the case with systems software and office productivity packages, off-the-shelf software will be purchased. Where the business has more specific needs and wishes to achieve a competitive advantage, bespoke and tailored approaches to acquisition will be used. With e-business systems there is often a need to integrate in-house legacy systems and systems purchased from different vendors. This uses a building block approach of different components including data sources that are integrated together. This is referred to as enterprise application integration (EAI), and achieving this is a significant challenge facing project managers and systems designers.

7.4 Factors affecting software acquisition

There are a number of factors that will influence the choice of acquisition method. Three critical ones are time, cost and quality considerations. If an organisation has a pressing problem that requires a new information system quickly, it is probable that a package or tailored package will be sought. Similarly, an organisation that needs a 'quality systems solution' may well consider the packaged software route, especially if its requirements are straightforward. The different acquisition options have different strengths when considered in terms of the three critical criteria. Quality of the delivered product is considered from two respects: the number of bugs or errors found and the suitability of the software in meeting the requirements of the business user. Note that good quality in terms of the number of bugs that typically occur for packaged software may coincide with poor quality in terms of the business fit.

The benefit of packaged software occurs because the cost of developing and debugging the software is shared between more than one company. This results in lower costs and fewer bugs than bespoke development for a single company. The use of packaged software by more than one company is also its greatest weakness, since its features must suit the typical company. As a consequence, it may not meet the needs of an individual company. Other factors affecting software acquisition include the following:

- *Organisation size*. A small or medium-sized business will inevitably have relatively limited resources for the purchasing of information systems and information technology (IS/IT). This suggests that there will be a tendency for such organisations to favour the purchase of off-the-shelf packages or possibly end-user applications development.

- *In-house IS/IT expertise*. Where little in-house IS/IT expertise exists, either in the form of IS/IT professionals or experienced end-users, there will be a need to use third parties in the acquisition of new business information systems. These may include software vendors for off-the-shelf software packages, the use of consultants and/or software houses. Precisely what form of third party is used will depend on the other factors discussed here.

- *Complexity of the required information system*. Where a business information system requirement is particularly complex, or for an unusual application not available as a packaged solution, it is possible that one may view bespoke software (either developed in-house or by a third party) as the only viable solution. However, complexity does not necessarily equate to 'uniqueness'. For example, one could regard a materials requirements planning system or a complete accounting system as complex, but many packages exist for a variety of hardware platforms. Therefore, complexity is not necessarily an indicator that an off-the-shelf package should be ruled out.

- *Uniqueness of the business or business area to be supported*. The higher the degree of uniqueness that exists in the area to be supported, the less likely it is that a suitable off-the-shelf package can be found. This is clearly an indicator, therefore, for bespoke development of some kind. As before, we must not confuse uniqueness with complexity. It may well be feasible for a non-IS/IT specialist to develop a solution using tools available to end-user developers. Of course, if the required system is complex and also carries a high degree of uniqueness, then bespoke development by IS/IT professionals is probably the best acquisition method.

- IS/*IT expertise among end-users*. A certain degree of IS/IT literacy and expertise is necessary if end-users are to be able to develop information systems. In addition, such literacy is desirable when selecting suitable off-the-shelf packaged software, as it can help the business focus more clearly on its precise requirements from both a functional and a technological perspective. If an organisation has little end-user IS/IT expertise of its own, but has its own IS/IT department, it will be very much dependent on solutions provided by IS/IT professionals with or without third-party support.

- *Linkages with existing applications software*. Where new business software needs to integrate very tightly with existing information systems, there is a higher probability that at least some bespoke development work will need to be done to integrate the two systems. Also, a high degree of integration may imply that the new information system has to be developed in a bespoke fashion in order to achieve the desired level of integration. Having said that, many software vendors supply packages for different business areas which integrate very well with each other.

By looking at combinations of the above, it is possible to come up with a 'best-fit' acquisition method.

8 Developing Information Systems

8.1 The systems development life cycle

The systems development life cycle (SDLC) is the classical approach used to develop information systems (Kroenke, 2007). The SDLC approach recognises that systems are developed in a series of steps or phases and that each phase needs to be completed before the next one commences. Recognition is also given to the fact that the programming activity (part of the build phase) should only commence once user requirements have been determined and the system design produced. We will now summarise the basic steps that most systems development projects follow.

8.1.1 Initiation

Initiation phase is the initiation or startup phase and is the first phase in an information systems development project. Its aims are to establish whether the project is feasible and then prepare to ensure the project is successful. The initiation phase contains the stimulus from which the need to develop a new BIS arises. This stimulus may come about as a result of some external event such as a change in legislation, or it may arise from a desire internally to develop an information system that better supports the business needs of the organisation. The source of this initiation process may be one of the following:

- *Managing director or other senior management*. Systems initiated from this point are likely to have the support necessary for successful development.

- *Information systems department*. A system may be initiated here as part of the organisation's overall IS/IT strategy; to maximise the chances of success the system will still need high-level management support.

- *Functional business area*. A system initiated here will be competing for attention with all other development projects then being undertaken; often an organisation will have a steering committee to decide on development priorities.

8.1.2 Feasibility assessment

Feasibility assessment is the activity that occurs at the start of the project to ensure that the project is a viable business proposition. The feasibility report analyses the need for and impact of the system and considers different alternatives for acquiring software. The feasibility assessment can be considered to be part of the *initiation phase*. It will establish whether a computer-based information system fits certain feasibility criteria. Three criteria are usually cited:

- It must be established whether the information system is technically feasible. To be technically feasible, either the technology exists or it can be created to support the required system.

- To be economically feasible, an information system must generate more in the way of benefits than the cost needed to produce it. One of the problems here is that benefits are often difficult to quantify in monetary terms, while costs are far easier to estimate.

- Assuming that a proposed information system is both technically and economically feasible, an assessment must be made of whether the project is operationally and organisationally feasible. By operationally feasible, we mean that the system must be capable of performing within the required speed, volume, usability and reliability parameters. Also, to be feasible for the organisation, the proposed information system must either be capable of running alongside work patterns or existing work patterns must be capable of being adapted or re-engineered to run alongside the new information system. Organisational feasibility will involve a review of how the potential users' skill sets and attitudes will affect the system.

Part of the feasibility process may be the invitation to tender for some or all of the information system elements. These may include application software, hardware, communications technology or systems software. Different alternatives from different vendors will then be assessed.

The output from this step (and, therefore, the input to the next step of the model) is a stage review and a feasibility report, which will recommend either that the project proceeds or that the project is reassessed in some way.

8.1.3 Systems analysis

Systems analysis is the capture of the business requirements of a system from talking to or observing end-users and using other information sources such as existing system documentation. Once a proposed information system is agreed to be feasible, it is necessary to carry out the detailed work of assessing the precise requirements that the intended users have for the new system. Note that the systems analysis step is sometimes referred to as the 'requirements determination' step or the 'systems study' step. There are three main tasks within this phase.

First, it is necessary to gain an understanding of how the current information system (computerised or paper-based) works. Second, a diagrammatic model of the current system workings is produced to ensure that IT professionals and system users are in agreement. Finally, a set of requirements for the new information system is produced. The requirements specification will define:

- the features that the new system is required to contain (e.g. the ability for end-users to be able to design their own reports);
- the scope of the system under consideration (for example, is the system intended for just one functional area of the business or is it to embrace all business activities?);
- the intended users of the new system;
- system performance standards, including response times, batch processing times (if required) and reliability needs;
- environment requirements such as physical working environment, operating system and hardware on which the system will run. In this last task, it may be desirable to produce another diagrammatic model, this time of the required information system.

If at any point it is discovered that the requirements of the system as articulated by the prospective users appear to be unfeasible in some way, it will be necessary to revisit the feasibility step and perform an additional analysis of the possible options. The output from this step in the model will be a user requirements analysis document which details what the proposed system must do.

8.1.4 Systems design

The systems design phase defines how the system will work in key areas of user interface, program modules, security and database transactions. The input to this stage is a breakdown of the requirements that the proposed information system is to deliver. The task of the systems design stage is to convert those requirements into a number of design alternatives from which the best will be selected. The design step therefore deals with how the proposed information system will deliver what is required. Systems design deals with such matters as:

- choosing an appropriate database management system;
- establishing general systems security standards;
- deciding on methods of system navigation (e.g. menu systems and graphical user interfaces);
- general standards for printed report production;
- screen design standards for input and output;

- data capture requirements;
- data storage requirements.

Detailed design, on the other hand, will result in a blueprint for individual system modules which will be used in the systems build phase that follows. Detailed design will further define some of the aspects of system design referred to above. If at any point during the design step it becomes obvious that the requirements as presented in the analysis step do not have a design solution (e.g. because of conflicting or incomplete requirements), it will be necessary to revisit the analysis step and determine more precisely what the new information system is to do in those particular respects.

8.1.5 System build

System build is the creation of software by programmers. It involves writing the software code (programming), building release versions of the software, constructing and populating the database and testing by programmers and end-users. Writing of documentation and training may also occur at this stage. The term 'build' is one that we shall be using in addition to the more usual and ambiguous term 'implementation' which is found in many texts and methodologies. This step embraces three substeps: physical database construction, programming and testing.

Physical database construction involves the conversion of the database design from the previous step into the required tables and indexes of a relational database. The programming substep involves the construction of computer code that will handle data capture, storage, processing and output. In addition, it will be necessary to program various other operational attributes of the required system (e.g. those that stem from control design). Alongside and subsequent to the programming substep, various forms of testing will take place. The output from the build stage will be an information system that has been tested and is available for final data conversion or take-on and live operation. If during the build phase it appears from testing that the system does not meet the original requirements as determined during the analysis step, then it will be necessary to revisit the design step to see whether any errors were made in interpreting the systems requirements. If the design brief was correctly interpreted but the system still contains errors in the delivery of the perceived requirements, it will be necessary to revisit the analysis to determine the systems requirements more precisely.

8.1.6 System implementation and changeover

System implementation covers practical issues such as making sure the hardware and network infrastructure for a new system are in place; testing of the system; and also human issues of how best to educate and train staff who will be using or affected by the new system. Implementation also involves the transition or changeover from the old system to the new. This step in the waterfall model deals with preparing for and making the change from old to new information systems. As one might expect, the systems implementation step is fraught with difficulties. Here, it will be discovered whether all the previous steps have combined to deliver an information system that does what the users actually want and that also works properly. Data will be converted from old information systems or directly entered into the new database. Finally, the new system will become operational straight away, or in phases, or after a period of parallel running. If errors are encountered at the live running stage it may be possible for the system to continue in operation while the errors are corrected. Alternatively, it may be necessary to suspend the operation of the new system while the most significant errors are fixed. Such error correction may require any of the previous steps to be revisited, depending on the nature and severity of the error(s). It will be clear from this short discussion that the later in the systems development process errors are discovered, the higher is the cost of putting them right. The worst-case scenario is probably for a system to have reached the live running stage only for it to be discovered that the required system was never really feasible in the first place.

8.1.7 Review and maintenance

Once an information system is operating under live running conditions, it will be inevitable that changes will be required over time. The maintenance phase involves two different types of maintenance. The first, known as 'unproductive maintenance', stems from errors or oversights in the original systems development which, while not preventing the system operating to an acceptable level, are still necessary to correct for it to conform with the original specification. The second form of maintenance involves the addition of new features and facilities that extend the scope and functionality of the information system. In the early days, these may take the form of 'nice-to-haves' or 'bells and whistles' which were not deemed to be essential to the system at changeover time. Over the longer term, the system will be adapted and modified to meet changing business requirements. An activity known as the post-implementation review should also be undertaken. This should take place about six months after the system changeover and should review what was planned for the information system against what actually happened. Lessons learned from this exercise will be extremely valuable when the next system is developed.

9 Systems Development Methodologies

9.1 SSADM

Structured Systems Analysis and Design Method (SSADM) is a structured development method that was developed initially in the 1980's as a public domain standard development method (Beynon-Davies, 2009). SSADM focuses on the feasibility, analysis and design aspects of the systems development life cycle. It provides fewer guidelines on the changeover and maintenance aspects of an IS project. Describing SSADM in some detail highlights the methodical approach required for large-scale projects which some may refer to as bureaucratic. It also illustrates the contrast with alternative techniques such as RAD. SSADM has a five-module framework within which are seven stages. The five modules are now discussed.

9.1.1 Feasibility Study

The project will already have been through a planning or initiation stage, so it is necessary at this point to determine whether it is technically and economically feasible. The feasibility study is broken down into four steps:

- *prepare for feasibility study* by assessing the scope of the project;
- *define the problem* (what should the new system do that the present one does not);
- *select the best feasibility option* from those available (typically up to five business options and a similar number of technical options);
- *assemble the feasibility report*, including a rationale for the selected option.

The output from this stage, the feasibility report, now provides the input for the next module; requirements analysis.

9.1.2 Requirements Analysis

This stage is critically important because it is used to gain a full understanding of what is required of the new system. Any errors or omissions made at this stage will be reflected in the rest of the systems development process. The following steps are taken:

- *Establish analysis framework*. The scope of the project is reassessed and then planned accordingly.
- *Investigate and define requirements*. Broad requirements will have been defined at the feasibility stage: these are now expanded into a detailed catalogue of systems requirements.
- *Investigate current processing*. The feasibility study will have created an initial data flow diagram which is now expanded to embrace all the existing processes.

- *Investigate current data*. A logical data model is developed so that the organisation can obtain a clear picture of which attributes the data entities contain and how they relate to each other.

- *Derive logical view of current services*. This involves the revision of the logical data model so that it reflects the business logic of the system under consideration rather than its current physical implementation.

- *Assemble investigation results*. This is the last step in the analysis of the current system environment. The analysts will check for consistency and completeness before proceeding to the next stage.

A number of possible systems solutions for the perceived business requirements are formulated and the impacts and benefits of each will be evaluated. The solution selected will be the one that most closely matches the requirements of the business. The two steps are:

- *Define business systems options*. Activities here will include the establishment of minimum systems requirements, the development in skeleton form of alternatives, the production of a short list of options, and finally a full evaluation of each alternative short-listed option, including a cost–benefit analysis, impact analysis and system development and integration plan for each.

- *Select business system option*. The precise way in which this is done will vary between organisations. The objective is the same, however: for appropriate user managers to select the business system option from the evidence presented by the analysis team.

9.1.3 Requirements specification

This module has one stage which in turn is split into eight discrete steps.

- *Define required system processing*. Here, the features of the existing system that are to remain a part of the new system are added to the details contained in the requirements catalogue.

- *Develop required data model*. Redundant elements from the data model of the existing system are removed (if any exist) and additional required elements are added. In addition, the relationships between old and new entities are reviewed.

- *Derive system functions*. Here, the processes that will have been identified and incorporated in the data flow diagrams are identified more precisely and properly documented.

- *Enhance required data model*. The required data model developed earlier is now enhanced by carrying out relational data analysis and normalisation; the result should be a set of tables which can be implemented using a relational database management system.

- *Develop specification prototypes*. This involves the creation of prototypes for selected parts of the specification so that precise requirements can be validated with the intended end-users; such elements as menus, sample data entry screens and reports may be constructed.

- *Develop processing specifications*. The analyst at this stage is concerned with illustrating the effect of time on data subjected to various actions (i.e. creation, reading, updating and deleting); two tools that are used here are entity life history analysis and effect correspondence diagrams. These are tools used by the professional systems analyst and it is beyond the scope of this book to deal with them in detail.

- *Confirm system objectives*. The penultimate task is to carry out a formal review of the system requirements to ensure that the final requirements specification which follows is complete and fully understood by users and developers alike.

- *Assemble requirements specification*. Finally, the various components (including the required system logical data model, function definitions, requirements catalogue and other items) are assembled into the final requirements specification document, which then provides the input into the next module and stage.

9.1.4 Logical system specification

Here, any constraints on the choice of technical environments are established (e.g. security, performance, ease of upgrade). The appropriate technical option is selected; it must conform with the required strategic and operational criteria which have already been established. The process of developing the systems specification is continued, with the outcome being a set of implementable components. The individual steps are as follows:

- *Define user dialogues*. This is concerned with defining the ways in which the user will interact with the system (e.g. menus and systems navigation).

- *Define update processes*. Here, the definition of transactions which will change data are established (entity life histories are used to support this step).

- *Define enquiry processes*. In addition to navigation and updating, users will wish to perform enquiries on the data held in the system.

- *Assemble logical design*. This is essentially a consistency and completeness check. Once the logical design is complete and has been 'signed off', the final stage can be tackled.

9.1.5 Physical design

This stage is concerned with the delivery of the final blueprint from which the system can be developed and implemented. There are seven steps to be completed:

- *Prepare for physical design*. The implementation environment is studied, applications development standards drawn up and a physical design strategy agreed.

- *Create physical data design*. The required logical data model (LDM) is used as a base for this and the business-specific data design is produced.

- *Create function component implementation map*. The components of each systems function are drawn up. This includes their relationship with the physical function components (the actual business activities) which they support.

- *Optimise physical data design*. The physical data design is tested against the required performance objectives and optimised if necessary.

- *Complete function specification design*. This will be for any function components that required programming.

- *Consolidate process data interface*. The process data interface is located between the physical database design and the process design. This helps the mapping of the database to the processing requirements (especially important when the database has been altered or the processing requirements have been modified).

- *Assemble physical design*. This stage and the whole SSADM lifecycle are completed with this step. A number of products are delivered, including the function definitions, the optimised physical data design, the requirements catalogue and space and timing estimates.

9.2 Rapid applications development (RAD)

The evidence from project failures for projects in the 1980s and 1990s implies that traditional structured methodologies have a tendency to deliver systems that arrive too late and therefore no longer meet their original requirements. Traditional methods can fail in a number of ways:

- *A gap of understanding between users and developers*. Users tend to know less about what is possible and practical from a technology perspective, while developers may be less aware of the underlying business decision-making issues which lie behind the systems development requirement.

- *Tendency of developers to isolate themselves from users*. Historically, systems developers have been able to hide behind a wall of jargon, thus rendering the user community at an immediate disadvantage when discussing IS/IT issues. While some jargon may be necessary if points are to be made succinctly, it is often used to obscure poor progress with a particular development project. The tendency for isolation is enhanced by physical separation of some computer staff in their own air-conditioned computer rooms. Developers might argue in their defence that users also have their own domain-specific jargon which adds to the problem of deciphering requirements.

- *Quality measured by closeness of product to specification*. This is a fundamental difficulty – the observation that 'the system does exactly what the specification said it would do' hides the fact that the system may still not deliver the information that the users need for decision-making purposes. The real focus should be on a comparison of the deliverables with the requirements, rather than of deliverables with a specification that was a reflection of a perceived need at a particular point in time.

- *Long development times*. A glance back at the previous section on SSADM and the waterfall model will reveal that the processes of analysis and design can be very laborious and time consuming. Development times are not helped by the fact that an organisation may be facing rapidly changing business conditions and requirements may similarly be changing. There is a real risk of the 'moving goal-posts' syndrome causing havoc with a traditional approach to systems development.

- *Business needs change during the development process*. This is alluded to above. A method is needed where successive iterations in the development process are possible so that the latest requirements can be incorporated.

- *What users get isn't necessarily what they want*. The first a user may see of a new information system is at the testing or training stage. At this point, it will be seen whether the system as delivered by the IS/IT professionals is what the user actually needs. An appropriate analogy here is the purchase of a house or car simply on the basis of discussions with an estate agent or a garage, rather than by actually visiting the house or driving the car. It is unlikely that something purchased in this way will result in a satisfied customer and there is no reason to suppose that information systems developed in a similar way will be any more successful.

Not only is there pressure from end-user management for faster systems development, IS/IT departments themselves increasingly recognise the need to make more effective use of limited human resources within their departments while at the same time quickly delivering systems that confer business benefits. All this is in a climate of rapid business change and, therefore, rapidly changing information needs. Rapid applications development (RAD) is a possible solution to these problems and pressures. This uses prototyping to involve users and increase development speed. Rapid applications development (RAD) is a method of developing information systems which uses prototyping to achieve user involvement and faster development compared to traditional methodologies such as SSADM. Prototyping produces a preliminary version of part or a framework of all of an information system which can be reviewed by end-users. Prototyping is an iterative process where users suggest modifications before further prototypes and the final information system are built.

9.3 The spiral model

The spiral model is an iterative systems development model developed by Boehm (1988) which incorporates risk assessment. The spiral model was developed in recognition of the fact that systems development projects tend to repeat the stages of analysis, design and code as part of the prototyping process. Each spiral consists of four main activities which are:

- *Planning*. Setting project objectives, defining alternatives.
- *Risk analysis*. Analysis of alternatives and the identification and solution of risks.
- *Engineering*. Equivalent to the build phase of the SDLC with coding and testing.
- *Customer evaluation*. Testing of the product by customers.

The model is closely related to RAD, since it implies iterative development with a review possible after each iteration or spiral, which corresponds to the production of one prototype or incremental version. Before the first spiral starts the requirements plan is produced, so it can be seen that the spiral model does not detail the initiation and analysis phase of the SDLC, focusing on design and build. Although the spiral model has not been applied widely in industry, proponents of this model argue that it includes the best features of both the classic SDLC and the prototyping approach. It also adds validation of requirements and design, together with risk analysis, which is often overlooked in RAD projects.

9.4 The Capability Maturity Model

Another influential model for best practice in the development of BIS is the Capability Maturity Model for Software. This model, which has been revised throughout the 1990s and into the new millennium, challenges organisations to review their process of systems development. It provides a framework for managers to assess the current sophistication of their process for systems development. There are five stages to the model. These are described by the institute as:

- *Initial*. The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
- *Repeatable*. Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
- *Defined*. The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

- *Managed*. Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

- *Optimizing*. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

10 Information Systems Security

The role of computer controls and security is to protect systems against accidental mishaps and intentional theft and corruption of data and application, as well as to help organisations ensure that their IT operations comply with the law and with expectations of employees and customers for privacy (Oz and Jones, 2008). This section discusses security threats to information systems before introducing methods to protect information systems against these threats. A particular emphasis is placed on the areas of computer viruses and threats to Internet services.

10.1 Security Threats to Information Systems

Controls upon information systems are based upon the two underlying principles of the need to ensure the accuracy of the data held by the organisation and the need to protect against loss or damage. The most common threats faced by organisational information systems can be placed into the following categories of accidents, natural disasters, sabotage (industrial and individual), vandalism, theft, unauthorised use (hacking) and computer viruses which will now be described.

10.1.1 Accidents

A number of estimates suggest that 40–65% of all damage caused to information systems or corporate data arises as a result of human error. Some examples of the ways in which human errors can occur include:

- *Inaccurate data entry*. As an example, consider a typical relational database management system, where update queries are used to change records, tables and reports. If the contents of the query are incorrect, errors might be produced within all of the data manipulated by the query. Although extreme, significant problems might be caused by adding or removing even a single character to a query.

- *Attempts to carry out tasks beyond the ability of the employee*. In smaller computer-based information systems, a common cause of accidental damage involves users attempting to install new hardware items or software applications. In the case of software applications, existing data may be lost when the program is installed or the program may fail to operate as expected.

- *Failure to comply with procedures for the use of organisational information systems*. Where organisational procedures are unclear or fail to anticipate potential problems, users may often ignore established methods, act on their own initiative or perform tasks incorrectly.

- *Failure to carry out backup procedures or verify data backups*. In addition to carrying out regular backups of important business data, it is also necessary to verify that any backup copies made are accurate and free from errors.

10.1.2 Natural disasters

All information systems are susceptible to damage caused by natural phenomena, such as storms, lightning strikes, floods and earthquakes. In Japan and the United States, for example, great care is taken to protect critical information systems from the effects of earthquakes. Although such hazards are of less concern in much of Europe, properly designed systems will make allowances for unexpected natural disasters.

10.1.3 Sabotage

With regard to information systems, sabotage may be deliberate or unintentional and carried out on an individual basis or as an act of industrial sabotage. Individual sabotage is typically carried out by a disgruntled employee who wishes to exact some form of revenge upon their employer. The logic bomb (sometimes known as a 'time bomb') is a well-known example of how an employee may cause deliberate damage to the organisation's information systems. A logic bomb is a destructive program that activates at a certain time or in reaction to a specific event. In most cases, the logic bomb is activated some months after the employee has left the organisation. This tends to have the effect of drawing suspicion away from the employee. Another well-known example is known as a back door. The back door is a section of program code that allows a user to circumvent security procedures in order to gain full access to an information system. Although back doors have legitimate uses, such as for program testing, they can also be used as an instrument of sabotage. It should be noted, however, that individual sabotage is becoming more infrequent due to legislation such as the Computer Misuse Act.

Industrial sabotage is considered rare, although there have been a number of well-publicised cases over the past few years. Industrial sabotage tends to be carried out for some kind of competitive or financial gain. The actions of those involved tend to be highly organised, targeted at specific areas of a rival organisation's activities, and supported by access to a substantial resource base. Industrial sabotage is considered more serious than individual sabotage since, although occurrences are relatively few, the losses suffered tend to be extremely high. An intent to cause loss or damage need not be present for sabotage to occur. Imagine the case of an organisation introducing a new information system at short notice and without proper consultation with staff. Employees may feel threatened by the new system and may wish to avoid making use of it. A typical reaction might be to enter data incorrectly in an attempt to discredit the new system. Alternatively, the employee might continue to carry out tasks manually (or with the older system), claiming that this is a more efficient way of working. In such cases, the employee's primary motivation is to safeguard their position the damage or loss caused to the organisation's information systems is incidental to this goal.

10.1.4 Vandalism

Deliberate damage caused to hardware, software and data is considered a serious threat to information systems security. The threat from vandalism lies in the fact that the organisation is temporarily denied access to some of its resources. Even relatively minor damage to parts of a system can have a significant effect on the organisation as a whole. In a small network system, for example, damage to a server or shared storage device might effectively halt the work of all those connected to the network. In larger systems, a reduced flow of work through one part of the organisation can create bottlenecks, reducing the overall productivity of the entire organisation. Damage or loss of data can have more severe effects since the organisation cannot make use of the data until it has been replaced. The expense involved in replacing damaged or lost data can far exceed any losses arising from damage to hardware or software. As an example, the delays caused by the need to replace hardware or data might result in an organisation's being unable to compete for new business, harming the overall profitability of the company. In recent years, vandalism has been extended to the Internet. A number of incidents have occurred where company web sites have been defaced.

10.1.5 Theft

As with vandalism, the loss of important hardware, software or data can have significant effects on an organisation's effectiveness. Theft can be divided into two basic categories: physical theft and data theft. Physical theft, as the term implies, involves the theft of hardware and software. Data theft normally involves making copies of important files without causing any harm to the originals. However, if the original files are destroyed or damaged, then the value of the copied data is automatically increased. Service organisations are particularly vulnerable to data theft since their activities tend to rely heavily upon access to corporate databases. Imagine a competitor gaining access to a customer list belonging to a sales organisation. The immediate effect of such an event would be to place both organisations on an essentially even footing. However, in the long term, the first organisation would no longer enjoy a competitive edge and might, ultimately, cease to exist. Both data theft and physical theft can take a number of different forms. As an example, there has been growing concern over the theft of customer information, such as credit card details, from company web sites.

10.1.6 Unauthorised use

One of the most common security risks in relation to computerised information systems is the danger of unauthorised access to confidential data. Contrary to the popular belief encouraged by the media, the risk of hackers, gaining access to a corporate information system is relatively small. Most security breaches involving confidential data can be attributed to the employees of the organisation. In many cases, breaches are accidental in that employees are unaware that particular sets of information are restricted. Deliberate breaches are typically the result of an employee's wishing to gain some personal benefit from using the information obtained. However, we must consider that the threat posed by hackers is starting to increase as more organisations make use of the Internet for business purposes. In addition, it should be noted that even a relatively small number of hacking incidents can account for significant losses to industry.

A hacker is a person who attempts to gain unauthorised access to a computer-based information system, usually via a telecommunications link. However, this is the popular use of this term and is considered incorrect by many IT professionals. Traditionally, 'hacking' referred to the process of writing program code, so hackers were nothing more than skilled computer programmers. Even today, many people consider themselves to be 'hackers' of the traditional kind and dislike being associated with the stereotype of a computer criminal. Furthermore, many people draw distinctions between those who attempt to gain unauthorised access to computer-based information systems for malicious reasons and those with other motivations. A person who gains access to an information system for malicious reasons is often termed a cracker rather than a hacker. Similarly, many people claim to use hacking for ethical purposes, such as helping companies to identify security flaws or assisting law enforcement agencies in apprehending criminals. In general, most people consider hackers to fall into one of three categories of those who wish to demonstrate their computer skills by outwitting the designers of a particular system, those who wish to gain some form of benefit (usually financial) by stealing, altering or deleting confidential information and those who wish to cause malicious damage to an information system, perhaps as an act of revenge against a former employer. Understandably, the most common crime committed by hackers involves telecommunications fraud. Clearly, the first task carried out by most hackers is to obtain free telephone calls, so that the time-consuming task of breaking into a given system can be carried out without incurring a great deal of expense. However, the growth of digital communications technology means that it is possible to implement countermeasures against hacking.

10.1.7 Computer viruses

There are several different types of computer virus. Some examples include:

- The *link virus* attaches itself to the directory structure of a disk. In this way, the virus is able to manipulate file and directory information. Link viruses can be difficult to remove since they become embedded within the affected data. Often, attempts to remove the virus can result in the loss of the data concerned.

- *Parasitic viruses* insert copies of themselves into legitimate programs, such as operating system files, often making little effort to disguise their presence. In this way, each time the program file is run, so too is the virus. Additionally, the majority of viruses are created as terminate and stay resident (TSR) programs. Once activated, the virus remains in the computer's memory performing various operations in the background. Such operations might range from creating additional copies of itself to deleting files on a hard disk.

- *Macro viruses* are created using the high-level programming languages found in e-mail packages, web browsers and applications software, such as word processors. Technically, such viruses are extremely crude but are capable of causing a great deal of damage.

With the possible exception of anti-viruses (described in more detail later), all viruses must be considered to be harmful. Even if a virus program does nothing more than reproduce itself, it may still cause system crashes and data loss. In many cases, the damage caused by a computer virus might be accidental, arising merely as the result of poor programming. There is also evidence to suggest that viruses may be capable of causing physical damage to hardware components. It is possible, for example, to construct a virus that instructs a disk controller to attempt to read a non-existent track, causing immediate and irreparable damage to the hard disk drive. Until quite recently, it was thought that computer viruses could not be attached to data files, such as word processing documents or e-mail messages. However, the built-in programming languages featured within many modern applications mean that data files may now be used to transmit viruses. However, it remains true that viruses cannot be transmitted by a conventional e-mail message. A virus can only be transmitted as an attachment to a message, or if the e-mail package being used allows active content. Two other kinds of programs are related to computer viruses; worms and Trojans. A worm is a small program that moves through a computer system randomly changing or overwriting pieces of data as it moves. A Trojan appears as a legitimate program in order to gain access to a computer system. Trojans are often used as delivery systems for computer viruses.

10.2 Reducing the Threat to Information Systems

In general, there are four major approaches that can be taken to ensure the integrity of an information system. These are containment, deterrence, obfuscation and recovery. Although each strategy is discussed separately, it is important to note that an effective security policy will draw upon a variety of concepts and techniques.

10.2.1 Containment

The strategy of containment attempts to control access to an information system. One approach involves making potential targets as unattractive as possible. This can be achieved in several ways but a common method involves creating the impression that the target information system contains data of little or no value. It would be pointless, for example, attempting to steal data that had been encrypted the data would effectively be useless to anyone except the owner. A second technique involves creating an effective series of defences against potential threats. If the expense, time and effort required to gain access to the information system is greater than any benefits derived from gaining access, then intrusion becomes less likely. However, defences must be continually improved and upgraded in order to keep up with advances in technology and the increasing sophistication of hackers. Thus, such as approach tends to be expensive in terms of organisational resources. A third approach involves removing the target information system from potential threats. Typical ways in which this might be achieved include distributing assets across a large geographical area, distributing important data across the entire organisation or isolating important systems.

10.2.2 Deterrence

A strategy based upon deterrence uses the threat of punishment to discourage potential intruders. The overall approach is one of anticipating and countering the motives of those most likely to threaten the security of the system. A common method involves constantly advertising and reinforcing the penalties for unauthorised access. It is not uncommon, for example, to dismiss an employee for gaining access to confidential data. Similarly, it is not uncommon for organisations to bring private prosecutions against those who have caused damage or loss to important information systems. Attempts to breach the security of the information system are discouraged by publicising successful actions against employees or other parties. A second approach involves attempting to detect potential threats as early as possible, for example by monitoring patterns of information system usage and investigating all anomalies. However, although such a technique can prevent some attacks and reduce the damage caused by others, it can be expensive in terms of organisational resources. The third technique used commonly involves predicting likely areas of attack and then implementing appropriate defences or countermeasures. If an organisation feels, for example, that it is particularly vulnerable to computer viruses, it might install virus scanning software across the entire organisation.

10.2.3 Obfuscation

Obfuscation concerns itself with hiding or distributing assets so that any damage caused can be limited. One means by which such a strategy can be implemented is by monitoring all of the organisation's activities, not just those related to the use of its information systems. This provides a more comprehensive approach to security than containment or deterrence since it also provides a measure of protection against theft and other threats. A second method involves carrying out regular audits of data, hardware, software and security measures. In this way, the organisation has a more complete overview of its information systems and can assess threats more accurately. A regular software audit, for example, might result in a reduction in the use of illegal software. In turn, this might reduce the number of virus infections suffered by the organisation, avoid potential litigation with software companies and detect illegal or unauthorised use of programs and data.

The dispersal of assets across several locations can be used to discourage potential intruders and can also limit the damage caused by a successful attack. The use of other techniques, such as backup procedures, can be used to reduce any threats further.

10.2.4 Recovery

A strategy based upon recovery recognises that, no matter how well defended, a breach in the security of an information system will eventually occur. Such a strategy is largely concerned with ensuring that the normal operation of the information system is restored as quickly as possible, with as little disruption to the organisation as possible. The most important aspect of a strategy based upon recovery involves careful organisational planning. The development of emergency procedures that deal with a number of contingencies is essential if a successful recovery is to take place. In anticipating damage or loss, a great deal of emphasis is placed upon backup procedures and recovery measures. In large organisations, a backup site might be created, so that data processing can be switched to a secondary site immediately in the event of an emergency. Smaller organisations might make use of other measures, such as RAID facilities or data warehousing services.

10.3 Types of controls

There are five major categories of controls that can be applied to information systems. These are: physical protection, biometric controls, telecommunications controls, failure controls and auditing.

10.3.1 Physical protection

Physical protection involves the use of physical barriers intended to protect against theft and unauthorised access. The reasoning behind such an approach is extremely simple: if access to rooms and equipment is restricted, risks of theft and vandalism are reduced. Furthermore, by preventing access to equipment, it is less likely that an unauthorised user can gain access to confidential information. Locks, barriers and security chains are examples of this form of control.

10.3.2 Biometric controls

These controls make use of the unique characteristics of individuals in order to restrict access to sensitive information or equipment. Scanners that check fingerprints, voice prints or even retinal patterns are examples of biometric controls. Until relatively recently, the expense associated with biometric control systems placed them out of reach of all but the largest organisations. In addition, many organisations held reservations concerning the accuracy of the recognition methods used to identify specific individuals. However, with the introduction of more sophisticated hardware and software, both of these problems have been largely resolved. Many organisations have now begun to look at ways in which biometric control systems can be used to reduce instances of fraud.

10.3.3 Telecommunications controls

These controls help to verify the identity of a particular user. Common types of communications controls include passwords and user validation routines.

10.3.4 Failure controls

Failure controls attempt to limit or avoid damage caused by the failure of an information system. Typical examples include recovery procedures and regular backups of data. Backups are explained in more detail later on.

10.3.5 Auditing

Auditing involves taking stock of procedures, hardware, software and data at regular intervals.

With regard to software and data, audits can be carried out automatically with an appropriate program. Auditing software works by scanning the hard disk drives of any computers, terminals and servers attached to a network system. As each hard disk drive is scanned, the names of any programs found are added to a log. This log can then be compared to a list of the programs that are legitimately owned by the organisation. Since the log contains information concerning the whereabouts of each program found, it is relatively simple to determine the location of any unauthorised programs. In many organisations, auditing programs are also used to keep track of software licences and allow companies to ensure that they are operating within the terms of their licence agreements.

10.3.6 Detecting and preventing virus infection

The risk of virus infection can be reduced to a minimum by implementing a relatively simple set of security measures:

- unauthorised access to machines and software should be restricted as far as possible;
- machines and software should be checked regularly with a virus detection program;
- all new disks and any software originating from an outside source should be checked with a virus detection program before use;
- floppy disks should be kept write-protected whenever possible since it is physically impossible for a virus to copy itself to a write-protected disk;
- regular backups of data and program files must be made in order to minimise the damage caused if a virus infects the system.

Virus scanners are intended to detect and then safely remove virus programs from a computer system. The most common method of detection used by these programs involves scanning for the signatures of particular viruses. It is often possible to locate a virus by simply searching every file on an infected disk for these identifying characteristics. However, since new viruses are discovered quite frequently, the list of signatures contained within a detection program quickly becomes dated. For this reason, most software developers insist that regular program updates are essential. However, the introduction of new kinds of viruses, such as polymorphic and stealth viruses, mean that signature checking alone can no longer be regarded as a completely secure method of detection. For this reason, most virus scanners use a combination of techniques to enhance their efficiency. Amongst the methods used are checksums, virus shields, anti-viruses, heuristics and inoculation. Virus shields are TSR programs that constantly monitor and control access to a system's storage devices. Any unusual attempt to modify a file or write to a disk drive will activate a message asking the user to authorise the operation. A similar task is performed by hardware virus detection devices. Modern hardware protection devices can be extremely sophisticated, featuring their own processors, disk controllers and other expensive components. However, despite the claims of the manufacturers of these devices, there is little evidence to suggest that they are any more effective than software solutions. Once a virus has been detected there are three methods of removing it. The first, disinfection, attempts to restore damaged files and directory structures to their original condition. However, disinfection is not possible in all cases. The second technique involves overwriting the virus program so that it is permanently and irrevocably deleted from the disk. The third and final method of removing a virus is by restoring a backup of the infected disk to the system. The process of writing files to the disk effectively overwrites the virus and restores the system to its original state. Despite the sophistication of scanning programs, none is capable of offering complete protection against infection. Many tests have been carried out to determine the efficiency of specific virus-scanning programs. In all of these tests, no program has yet achieved a perfect score.

10.4 Techniques for controlling information systems

Some of the most common techniques used to control computer-based information systems are:

formal security policies, passwords, file encryption, organisational procedures governing the use of computer-based information systems, user validation techniques and backup procedures. The following describes each of these techniques in more detail.

10.4.1 Formal security policy

Perhaps the simplest and most effective control is the formulation of a comprehensive policy on security. Amongst a wide variety of items, such a policy will outline what is considered to be acceptable use of the information system, what is considered unacceptable use of the information system, the sanctions available in the event that an employee does not comply with the security policy and the details of the controls in place, including their form and function and plans for developing these further. Once a policy has been formulated, it must be publicised in order for it to become effective. In addition, the support of management is essential in order to ensure that employees adhere to the guidelines contained within the policy.

10.4.2 Passwords

The password represents one of the most common forms of protection for computer-based information systems. In addition to providing a simple, inexpensive means of restricting access to equipment and sensitive data, passwords also provide a number of other benefits. Amongst these are that access to the system can be divided into levels by issuing different passwords to employees based on their positions and the work they carry out. Also the actions of an employee can be regulated and supervised by monitoring the use of their password. Finally if a password is discovered or stolen by an external party, it should be possible to limit any damage arising as a result. The use of passwords can encourage employees to take some of the responsibility for the overall security of the system.

10.4.3 Encryption

An additional layer of protection for sensitive data can be provided by making use of encryption techniques. Modern encryption methods rely upon the use of one or more keys. Without the correct key, any encrypted data is meaningless and therefore of no value to a potential thief.

10.4.4 Organisational Procedures

Under normal circumstances, a set of procedures for the use of an information system will arise from the creation of a formal security policy. Such procedures should describe in detail the correct operation of the system and responsibilities of users. Additionally, the procedures should highlight issues related to security, should explain some of the reasoning behind them and should also describe the penalties for failing to comply with instructions.

10.4.5 User validation

Of relevance to telecommunications is the use of user validation techniques. It is necessary to verify the identity of users attempting to access the system from outside of the organisation. A password is insufficient to identify the user since it might have been stolen or accidentally revealed to others. However, by asking for a date of birth or other personal information, the identity of the user can be confirmed. Alternatively, if the location of the user is known, the system can attempt to call the user back at their current location. If the user is genuine, the call will be connected correctly and the user can then access the system. Although such methods do not offer total security, the risk of unauthorised access can be reduced dramatically.

10.4.6 Backup procedures

The effects of a sudden loss of data can affect a company's activities in a variety of ways. The disruption caused to a company's normal activities can result in significant financial losses due to factors such as lost opportunities, additional trading expenses and customer dissatisfaction.

The cumulative effects of data loss can prove detrimental to areas as diverse as corporate image and staff morale. Perhaps the single most compelling reason for introducing effective backup procedures is simply the expense involved in reconstructing lost data. One of the most common methods of protecting valuable data is to use the 'grand-father, father, son' technique. Here, a rotating set of backup disks or tapes are used so that three different versions of the same data are held at any one time. To illustrate this method, imagine a single user working with a personal computer and using three floppy disks to store their data on. Each day, all of the data being worked on is copied onto the disk containing the oldest version ('grandfather') of that data. This creates a continuous cycle that ensures that the oldest backup copy is never more than three days old. It is worth noting several general points concerning backups of data:

- The time, effort and expense involved in producing backup copies will be wasted unless they are made at regular intervals. How often backups are made depends largely upon the amount of work processed over a given period of time. In general, backups will be made more frequently as the number of transactions carried out each day increases.

- Backup copies of data should be checked each time they are produced. Faulty storage devices and media may sometimes result in incomplete or garbled copies of data. In addition, precautions should be taken against computer viruses, in order to prevent damage to the data stored.

- The security of backup copies should be ensured by storing them in a safe location. Typically, an organisation will produce two sets of backup copies; one to be stored at the company premises, the other to be taken off the premises and stored at a separate location. In this way, a major accident, such as a fire at the company premises, will not result in the total destruction of the organisation's data.

It is worth noting that not all data need be backed up at regular intervals. Software applications, for example, can normally be restored quickly and easily from the original media. In a similar way, if a backup has already been made of a given item of data, the production of additional copies may not be necessary. In order to reduce the time taken to create backup copies, many organisations make use of software that allows the production of incremental backups. Initially, a backup copy of all data files is made and care is taken to ensure the accuracy of the copy. This initial, complete backup is normally referred to as a full backup (sometimes also known as an archival backup). From this point on, specialised backup software is used to detect and copy only those files that have changed in some way since the last backup was made. In the event of data loss, damaged files can be replaced by restoring the full backup first, followed by the incremental backups. One of the chief advantages of creating incremental backups is that it is possible to trace the changes made to data files over time. In this way, any version of a given file can be located and restored.

10.5 Security Threats to Internet services

A number of significant new threats to organisational information systems have emerged connected to the increasing reliance on intranets and the Internet as basic tools for conducting transactions with partners, suppliers and customers. Although the following material focuses on the Internet, much of it is also relevant to company intranets.

10.5.1 Denial of service (DoS)

As companies begin to rely on network technology to reduce costs, they become more vulnerable to certain risks. For example, more harm can be caused if an individual gains access to a network server than if they merely gain access to a single PC. Similarly, companies relying on the Internet for business communications may find themselves subject to denial of service attacks. Typically, these attacks involve blocking the communications channels used by a company. For example, an e-mail system might be attacked by sending millions of lengthy messages to the company. Other techniques involve altering company web pages or attacking the systems used to process online transactions. In these cases, companies are usually forced to shut down services themselves until the problem can be dealt with. The impact of a denial of service attack can be extremely severe, especially for organisations that rely heavily on the Internet for e-commerce.

10.5.2 Trojans

Recently the use of Trojans to disrupt company activities or gain access to confidential information has grown sharply. Most of the Trojans encountered by business organisations are designed to gather information and transmit regular reports back to the owner. Typically, a Trojan will incorporate a key logging facility (sometimes called a 'keystroke recorder') to capture all keyboard input from a given computer. Capturing keyboard data allows the owner of the Trojan to gather a great deal of information, such as passwords and the contents of all outgoing e-mail messages. Some Trojans are designed to give owners control over the target computer system. Effectively, the Trojan acts as a remote control application, allowing the owner to carry out actions on the target computer as if they were sitting in front of it. Sometimes, the owner of the Trojan will make no effort to conceal their activities: the victim sees actions being carried out but is unable to intervene, short of switching off the computer. More often, however, the Trojan operates silently and the victim is unaware that their computer is running programs, deleting files, sending e-mail, and so on. Some programs are designed to disrupt company activities by initiating denial of service attacks or by attacking company servers. However, incidents involving these kinds of Trojan are rare since they often require very high levels of access to company systems.

10.5.3 Identity theft and brand abuse

Identity theft involves using another person's identity to carry out acts that range from sending libellous e-mail to making fraudulent purchases. It is considered relatively easy to impersonate another person in this way, but far harder to prove that communications did not originate from the victim. For business organisations, there is a threat that employees may be impersonated in order to place fraudulent orders. Alternatively, a company may be embarrassed if rumours or bogus press releases are transmitted via the Internet. The term brand abuse is used to cover a wide range of activities, ranging from the sale of counterfeit goods, for example software applications, to exploiting a well-known brand name for commercial gain. As an example, the name of a well-known company might be embedded into a special web page so that the page receives a high ranking in a search engine. Users searching for the name of the company are then likely to be diverted to the special web page where they are offered a competitor's goods instead.

10.5.4 Extortion

Various approaches can be used to extort money from companies such as cybersquatting and the threat of divulging customer information. Cybersquatting involves registering an Internet domain that a company or celebrity is likely to want to own. Although merely registering a domain is not illegal in itself, some individuals attempt to extort money from companies or celebrities in various ways. Typically, the owner of the domain will ask for a large sum in order to transfer the domain to the interested party. Sometimes, however, demands for money may be accompanied by threats, such as the threat the domain will be used in a way that will harm the victim's reputation unless payment is forthcoming. Although there is an established mechanism for dealing with disputes over domain names, many victims of cybersquatting choose not to use these procedures since they do not wish to attract negative publicity. A more common form of extortion usually occurs after a security breach in which sensitive company information has been obtained. Often, the threat involves making the information available to competitors or the public unless payment is made.

10.5.5 Abuse of resources

Organisations have always needed to ensure that employees do not take advantage of company resources for personal reasons. Whilst certain acts, such as sending the occasional personal e-mail, are tolerated by most companies, the increased availability of Internet access and e-mail facilities increases the risk that such facilities may be abused. Two examples of the risks associated with increased access to the Internet involve libel and cyberstalking. Cyberstalking is a relatively new form of crime that involves the harassment of individuals via e-mail and the Internet. Of interest to business organisations is the fact that many stalkers make use of company facilities in order to carry out their activities. There have also been cases of 'corporate stalking' where an organisation has used its resources to harass individuals or business competitors. For an organisation, the consequences of cyberstalking can include a loss of reputation and the threat of criminal and civil legal action.

10.5.6 Other risks

This section provides a discussion of two additional examples of emerging threats: cyberterrorism and stock fraud. Cyberterrorism describes attacks made on information systems that are motivated by political or religious beliefs. Organisations involved in the defence industries are often the victims of such attacks. However, many other companies are also at risk from politically motivated attacks. For example, companies trading in countries that are in political turmoil or companies with business partners in these countries also face the risk of such attacks. A number of recent cases have highlighted the danger of allowing inaccurate or misleading information to propagate across the Internet. Online stock fraud involves artificially increasing or decreasing the values of stocks by spreading carefully designed rumours across bulletin boards and chat-rooms. Whilst such activities may seem relatively harmless, companies can suffer significant losses. Incidences of online stock fraud highlight an extremely important issue: organisations are at risk from the distribution of false information across the Internet. It is important to note that the effects of online stock fraud are not limited only to influencing stock prices. Imagine, for example, what might happen if bogus press releases began to appear when a company was in the process of negotiating a merger or strategic alliance. Preventing inaccurate or misleading information from appearing on the Internet is fraught with difficulty. The sheer size of the Internet means that monitoring web sites, chat-rooms and news services places an unacceptable burden on the resources of even the largest organisations.

Bibliography

Benyon-Davies, P 2009, *Business Information Systems*, Palgrave Macmillan, Basingstoke.

Bocij, P; Greasley, A; Hickie, S 2008, Business Information Systems, 4th edn, Pearson Education, Harlow.

Kroenke, D.M 2011, *Using MIS*, 4th edn, Pearson Education, New Jersey.

Laudon, K.C & Laudon, J.P 2007, *Essentials of Business Information Systems*, 7th edn, Pearson Education, New Jersey.

Oz, E & Jones, A 2008, *Management Information Systems*, Cengage Learning, London.

Turban, E; Sharda, R; Delen, D 2010, *Decision Support and Business Intelligence Systems*, 9th edn, Pearson Education, New Jersey.